EXHIBIT 3

HAGENS BERMAN SOBOL SHAPIRO LLP
Shana E. Scarlett (Bar No. 217895)
shanas@hbsslaw.com
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
(510) 725-3000

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Kevin Y. Teruya (Bar No. 235916)
kevinteruya@quinnemanuel.com
865 South Figueroa Street, 10th Floor
Los Angeles, CA 90017-2543
(213) 443-3000

Interim Co-Lead Consumer Class Counsel

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MAXIMILLIAN KLEIN, *et al.*,

Plaintiffs,

v.

META PLATFORMS, INC., a Delaware Corporation headquartered in California

Defendant.

This Document Relates To: All Actions

Case No. 3:20-cv-08570-JD

Hon. James Donato

CONSUMER PLAINTIFFS' OBJECTIONS AND RESPONSES TO DEFENDANT META PLATFORMS, INC.'S FIFTH SET OF INTERROGATORIES TO USER PLAINTIFFS

produce information, documents, and things that are not in the possession, custody, or control of Consumer Plaintiffs.

SPECIFIC RESPONSES AND OBJECTIONS

INTERROGATORY NO. 22:

For each act, statement, and omission by or of Meta that You contend to be unlawful exclusionary conduct, including but not limited to any of the statements and omissions that You identified in Your response to Meta's Interrogatory No. 6 and any of the practices that You identified in Your response to Meta's Interrogatory No. 21, describe in full and complete detail (including but not limited to by identifying all facts, Documents, and witnesses that relate to Your contention) the basis for Your contention, if any, that such act, statement, or omission was "(1) clearly false, (2) clearly material, (3) clearly likely to induce reasonable reliance, (4) made to buyers without knowledge of the subject matter, (5) continued for prolonged periods, and (6) not readily susceptible of neutralization by rivals." *Am. Pro. Testing Serv., Inc. v. Harcourt Brace Jovanovich Legal & Prof. Publ., Inc.*, 108 F.3d 1147, 1152 (9th Cir. 1997).

RESPONSE TO INTERROGATORY NO. 22:

Consumer Plaintiffs object to this Interrogatory on the grounds set forth in detail above in their General Objections. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds it is entirely duplicative of Interrogatory Nos. 6-8, and 21. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds that it is overbroad, unduly burdensome, and disproportionate to the needs of the case, including in requesting that Consumer Plaintiffs "identify[] all facts, Documents, and witnesses that relate to [Consumer Plaintiffs'] contention." Consumer Plaintiffs do not agree to identify every fact, document, or witness that "relates" to Consumers' claims, and are not obligated to do so under the relevant Rules and law applicable to this case. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds and to the extent that due to Facebook's definition of "You" and "Your," the Interrogatory consequently (a) seeks irrelevant information not reasonably calculated to lead to the discovery of admissible evidence; (b) purports to require Consumer Plaintiffs to search for and provide information that is not in their

possession, custody, or control and/or to which Consumer Plaintiffs do not have access; and (c) includes Consumer Plaintiffs' legal counsel and attorneys and seeks to discover documents, data, or information protected by the attorney-client privilege, work product doctrine, the common interest privilege, and/or other investigative privileges or protections. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds and to the extent it requires the class representatives to draw a legal conclusion. Consumer Plaintiffs further specifically object to this Interrogatory to the extent that the Interrogatory seeks information that will necessarily be the subject of expert testimony and analysis. Consumer Plaintiffs will make expert disclosures and produce their expert reports pursuant to the schedule for expert discovery set by the Court.

Consumer Plaintiffs further specifically object to this Interrogatory to the extent that it purports to seek every document or all information that support or otherwise relates to specific contentions in this litigation, and that (a) Facebook continues to produce documents on a near-daily basis, and (b) depositions continue to occur on a daily basis, meaning that transcripts for many depositions have not yet been completed in final form. Consumer Plaintiffs have provided a proportionate response based on information reasonably available to them at this time, but reserve the right and ability to amend the responses after the close of fact discovery to incorporate further documents, facts and witness testimony.

Subject to and without waiving these objections, Consumer Plaintiffs respond as follows:

Consumer Plaintiffs incorporate by reference their Responses to Interrogatory Nos. 6-8, and 21, as if fully set forth herein. In addition to the Responses to those Interrogatories, the following is an additional, non-exhaustive, illustrative list of the acts, statements, and omissions of Facebook that Plaintiffs contend are relevant to their claims.

Facebook regularly collected and retained more consumer data than it disclosed, including instances when it apologized for data collection-related conduct. For instance, beginning on November 6, 2007, Facebook automatically opted all users into a project called Beacon, collecting off-platform online shopping activity. *See* Facebook, Leading Websites Offer Facebook Beacon for Social Distribution (Nov. 6, 2007), https://about.fb.com/news/2007/11/leading-websites-offer-

facebook-beacon-for-social-distribution/. On or around December 5, 2007, Mark Zuckerberg apologized for this action and publicly stated it was contrary to how Facebook would collect data moving forward. CONSUMER-FB-0000001205. Beacon was later disabled, but Mr. Zuckerberg's statement was untrue, as demonstrated by the below chart, which includes examples of why this was untrue.

Facebook's representation	**Facebook's action**
Facebook assured consumers that they had control over their profile and who their profile was shared with.	Facebook launched the Beacon feature, which displayed people's profile photos next to commercial messages shown to their friends about items they purchased or registered an opinion about.[1] But even when users opted out, Facebook was able to track them across the internet. The true purpose of Beacon was revealed in Facebook's behind-the-scene discussions with Beacon partners, including, *inter alia*: - eBay protested that the contract "needs to be completely re-done. We are NOT going to give you a perpetual license to do whatever you want to do with user data. Totally violates our privacy policy and user expectations. Also, we just don't let anybody do this sort of thing- not even those who have offered to pay for the privilege." Facebook's David Fischer said internally to his team, "I guess the take away here . . . is that we don't have time to be chasing rainbows at this point. The tradeoff just isn't worth it. We want dumb and desperate companies, not ones who understand the value of the data we are getting."[2] - Amazon pulled out of Beacon. Dan Rose, Facebook's VP of Partnerships, stated "Sounds like the mtg with Jeff might have caused him to realize that building apps will give us data that we could subsequently use against them (which is

[1] CONSUMER-FB-0000001854.

[2] PALM-003179321: 10/22/2007.

Facebook's representation	Facebook's action
	true -- we could ostensibly allow B&N to target ads at users who have added an Amazon app)."[3] - Facebook's Dave Morin says the "holy grail" for an agreement with Apple is: Apple would have iTunes app integration which allows FB to identify user by connecting FB account with iTunes, and have iTunes deliver "all song listening data to Facebook en masse."[4] - Travelocity stated they are "planning to hold off a month on launch because (CA article) data is sent regardless and we have to rely on FB to destroy it. This came up during contract negotiations and you told us it was "technical" and could not be fixed. We are hoping you can adjust the program to ensure no data is sent or no system ping occurs unless the member wants it sent. The challenge is to re-write our privacy policy to say 'your data is being sent regardless of what you may or may not want'."[5]
In its November 6, 2007 statement announcing the Beacon product, Facebook represented that: "In keeping with Facebook's philosophy of user control, Facebook Beacon provides advanced privacy controls so Facebook users can decide whether to distribute specific actions from participating sites with their friends." Facebook assured users that: "[w]hen users who are logged into Facebook a participating site, they receive a prompt asking whether to [sic] they want to share those activities with their friends on Facebook. If they do, those friends can now view those actions through News Feed or Mini-Feed stories." [6]	However, even if users opted out, Facebook could still track users across the internet: "[W]hen a user visited a Beacon site (e.g., blockbuster.com), regardless of whether the user consented or not, Facebook code initiated an HTTP request on behalf of the user to Facebook's servers. Through this newly opened connection, Facebook could write cookies on user computers during HTTP responses, or read cookies during HTTP requests. The requests and cookies could reveal the specific page a user was on—effectively allowing Facebook to accomplish surveillance on the users that had clicked 'No, Thanks.'[7]

[3] PALM-003251382: 10/04/2007.

[4] PALM-006445112: 10/30/2007.

[5] PALM-006442583.

[6] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002366; https://about.fb.com/news/2007/11/leading-websites-offer-facebook-beacon-for-social-distribution/.

[7] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002367.

Facebook's representation	Facebook's action
In a New York Times interview, Chamath Palihapitiya—Facebook's Vice President of Marketing—represented that Facebook would only receive information through Beacon *if* a user consented: Q. If I buy tickets on Fandango, and decline to publish the purchase to my friends on Facebook, does Facebook still receive the information about my purchase? A. "*Absolutely not*. One of the things we are still trying to do is dispel a lot of misinformation that is being propagated unnecessarily."[8]	Stefan Bertreau, a senior research engineer at California's Threat Research Group, examined the actual contents of Facebook's HTTP requests and responses," determining that Mr. "Palihapitiya's representations were not true.[9] After backlash, Mark Zuckerberg apologized for Beacon: "I'm not proud of the way we've handled this situation and I know we can do better."[10] Mr. Zuckerberg conceded, "that if someone forgot to decline to share something, Beacon still went ahead and shared it with their friends."[11] Several years after the Beacon debacle, on February 1, 2010, Facebook continued to make choices to limit users' ability to opt out sharing with their friends. In one discussion, Mike Vernal brought the concern "that showing recent activity in games / apps will be a pretty bad experience for some people. I don't think we can go to an opt-in model, but as a philosophy we should give people the tools to control the information they share." Naomi Gleit responds, "We made an explicit decision not to create a privacy setting for recent activity in general. Currently, there is a lot of user feedback that they want to control their non-platform related recent activity – however, we've pushed back on this because we want the flexibility to display these stories in fbx profile…"[12]

Facebook also failed to disclose that it tracked the off-platform activity of users and non-users, alike. For example, from 2010-2011, Facebook placed the Like Button on third-party websites

[8] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002366.

[9] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002367.

Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 57-58 (2019).

[10] CONSUMER-FB-0000001205.

[11] https://www.zdnet.com/article/zuckerberg-speaks-lessons-learned-from-beacon/.

[12] PALM-003837558-PALM-003837559, 2/1/2010.

and tracked non-users and users' off-platform activity using cookies. They launched this program in April 2010. CONSUMER-FB-0000002215. This practice was first publicly disclosed in December 2010. *See Arnold Roosendaal, Facebook Tracks and Traces Everyone: Like This!*, TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES NO. 03/2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563. Additional publications corroborated this discovery in May 2011. *See* Amir Efrati, *'Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), https://www.wsj.com/articles/SB10001424052748704281504576329441432995616. However, as detailed in the illustrative examples below, Facebook once again downplayed the practice and publicly stated that it would rectify the behavior when, in fact, it did not.

Facebook's representation	**Facebook's action**
Facebook initially failed to disclose the Like Button or social plugins in their privacy policy. When it did disclose, it represented that social plugins collected only what Facebook "needed to operate." Facebook represented that it only collected limited information from Facebook users.	Facebook gathered information beyond what it needed to operate, including data from non-Facebook users and logged-out Facebook users. As early as 2009, Facebook recognized it needed to "understand user behavior offsite"—without it, Facebook faced the risk of a "potential 'death spiral,'" even as Facebook recognized the "[s]ignificant privacy issues."[13] In April 2010, Facebook received a complaint from a WaPo reader and WaPo representative, stating "I sincerely resent the Washington Post's decision to link my Facebook account to my Washington Post account without my permission. When I went to the Post's website today, I was already logged-in to Facebook - so where today's Editor's Note says 'allow' in the first sentence, it should say 'force.'... Furthermore, the Post's decision to become partners with Facebook indicates to me that the Post is not serious about privacy. As the Post is undoubtedly aware, Facebook is intentionally obtuse when it comes to letting users control their privacy." A WaPo representative asked Facebook, "Can you point us to the best, fastest and easiest ways to opt out to showing up in the widget. I selected showing

[13] PALM-010934635: 4/13/2009.

Facebook's representation	Facebook's action
	updates to only myself and what I like still shows up in my friends' activity feed." Elliot Schrage responded internally: "The MUCH bigger point is to arm them with the righ[t] messaging - ie to make clear that WPOST gets NO data from facebook and that NOTHING is communicated back to the readers friends on facebook unless s/he takes an action." Osofsky: "I'm going to reorder the Q&A so that the first question is: What user data will Facebook share with sites integrating Social plugins? Facebook is not sharing any data with us. Social plugins pull information directly from Facebook and we do not have access to the data from Facebook unless the user has given us expressed consent." (PALM-005147416, 4/22/2010) In June 2010, FB employees discussed response to questions regarding Like button - Ari Schwartz: "2) We suggest being a little clearer on the purpose specification for collecting data… We're suggesting the words 'only use' rather than 'need'. 3) At the end you suggest that data retention of 90 days is 'standard industry practice.' Unfortunately there is no data retention industry standard today. Also, social plugins are somewhat unique, so it is hard to equate it to others in any case." (PALM-010051121) In November 2010, FB employees discussed the fact that users could not set certain privacy restrictions. Monica Horak: "There is no link to edit the privacy of the application in the new Application Settings design.... In the new design, the only thing a user can do is remove the app." David Goldblatt: "[T]here is the potential for a pretty strong blow back if we tell the user 'sorry, you can't restrict this content, nor can you see what the settings are for this content.' - and then letting users know this content will be exposed indefinitely (because we can't let them know about fbx profiles.)" . . . Okelola: "We still need to respect the user's privacy settings for who can see their content. This privacy is different from each individual photo / album / video / event since we don't want to make it easy for anyone to just scrape the graph and see all the events a user

Facebook's representation	Facebook's action
	has ever attended, all the photos they've uploaded, etc. The default privacy setting here is friends of friends (was previously everyone for a few apps) but was changed... I can't find the task that had the discussion for moving from everyone to fof. Here's an article I found regarding all of a user's events being visible via the graph api." Sjogren: "IMHO, the privacy settings for our core applications should be in the main privacy dashboard and not treated like other platform applications that have no equivalent privacy controls. We should add photos/events/notes/links/groups/videos as core content who's privacy you can customize." Goldblatt: "Where we put these settings, doesn't matter, they just need to exist." (PALM-006500954)
In a May 2011 interview with The Wall Street Journal, Facebook's CTO Bret Taylor noted that Facebook did not use cookies "for tracking and they're not intended for tracking," assuring that a "bug" relating to the tracking of non-Facebook users through the Like button had been discontinued.[14]	Independent researcher Arnold Roosendaal discovered in December 2010 that, contrary to Facebook's representation that no data was shared by mere presence of a Like button, "each time a Facebook user visited a site with a Like button, Facebook retrieved the user's Facebook website login cookies, which contained the user's unique identifying number, traceable to his or her real identity." Facebook also "retrieved the specific URL the user was on, which revealed the title of an article the user was reading or the name of the product a user was buying." "Roosendaal then demonstrated that Facebook used these open connections to write cookies and surveil the behavior of people that did not even have Facebook accounts."[15]

[14] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002375.

[15] Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES NO. 03/2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563.

Facebook's representation	Facebook's action
	The Wall Street Journal corroborated Roosendaal's finding in a May 18, 2011 piece entitled *"Like" Button Follows Web Users*.[16] A few days before the article, high-level employees were preparing for its publication. Dan Rose stated the current status: "WSJ has been working on a story for several weeks saying that we log user behavior via plugins . . . We want to be able to say to WSJ (and anyone else who asks) that we are not logging data from plugins. We *won't* say that we will never log, we just will say that we aren't logging. We will stop logging immediately (obviously). We need to be able to continue to do the things listed below by Vernal which are critical to the way that Platform works. Whatever we say and do can't restrict us from doing those things" below, Vernal lists the things they would like to continue doing: "If it's a meaningful/important give, we're ok saying that we won't use social plugin impression data with the following caveats: 1/ The user can opt-in to sharing their impression activity (e.g., reading articles). We don't actually think of this as impressions, but one could so want to explicitly flag this. 2/ We can use the impression data in aggregate. This includes everything from global (total # of impressions) to smaller sets (networks, friend-of-friend clusters, etc.) We wouldn't commit to this unless it was a substantial give, because I do think we lose some value in personalization here, but I think it's a reasonable trade-off."[17] The day before this article came out, on May 17, 2011, Bret Taylor messaged Zuckerberg: "There are over 10 billion like buttons served per day, so we can 'track' the sites our users visit in theory because we get an HTTP referrer from the sites that host them in addition to the Facebook cookie. We don't actually use this information in practice. We only use actual likes, and we only use the

[16] Amir Efrati, *'Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), https://www.wsj.com/articles/SB10001424052748704281504576329441432995616.

[17] PALM-016493752-PALM-016493756.

Facebook's representation	Facebook's action
	impression data in aggregate for analytics like CTR." . . . "We introduced a policy last May that says we delete social plugin logs after 90 days, but it keeps coming back (including a WSJ piece slated to come out imminently)." . . . "Likewise, we are not updating our privacy policy or any other binding documents so we have some flexibility to modify our implementation in the future if we choose to change our data needs as it relates to plugins, and we are being careful to speak in the present tense in all of our drafted statements and not making any future promises."[18] On May 16, 2011, a document is circulated to help prepare Sheryl Sandberg before she travels internationally. The document is titled "'Like Button' Scenarios" and confirms that Facebook records an impression log for non-Facebook users and non-logged-in Facebook users: "A normal impression log record is created (includes IP address, date, time, URL, browser type, country code etc.) as for any visit to facebook.com."[19]

Facebook also failed to disclose to users that their platform permitted third-party websites access to user data, and then misrepresented that it would rectify the conduct when it became public. For example, from 2010 through 2011, Facebook permitted third-party websites access to user data and activity through the Like Button, without informing users. They launched this program in April 2010. CONSUMER-FB-0000002215. The public discovered this behavior in December 2010. *See* Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, TILBURG LAW SCHOOL LEGAL STUDIES RESEARCH PAPER SERIES NO. 03/2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563. Additional publications corroborated this discovery in May 2011. *See* Amir Efrati, '*Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), https://www.wsj.com/articles/SB10001424052748704281504576329441432995616.

[18] PALM-016624372.

[19] PALM-010572315.

Facebook's representation	Facebook's action
Facebook initially failed to disclose the Like Button or social plugins in their privacy policy. When it did disclose, it represented that social plugins collected only what Facebook "needed to operate."	Facebook permitted third parties to access consumers' data extensively through social plugins,[20] recognizing the importance of tracking to revenue. As early as 2009, Facebook recognized it needed to "understand user behavior offsite"—without it, Facebook faced the risk of a "potential 'death spiral,'" even as Facebook recognized the "[s]ignificant privacy issues."[21]
When Facebook launched the "Like" button, its "Frequently Asked Questions" page said, "No data is shared about you when you see a social plug-in on an external website."[22] In a May 27, 2010 interview with NPR, Mark Zuckerberg stated "[t]here's this false rumor that's been going around which says that we're sharing private information with applications and it's just not true."[23]	In a September 27, 2010 document containing "Advertising Privacy Messaging" chart, "Main message…We don't share – and never sell – your personal information with advertisers…What do you think about behavioral targeting? We don't do behavioral targeting and we don't think following people around the web is the right way to show relevant ads…How is what you do different from BT? Unlike most companies on the web, we don't target ads to you based on surveillance data from your actions across the web. We only use what you share or do on Facebook…What do you think about cookies?...we don't use cookie data based on web browsing behavior to [target] ads. We believe that we are the only major website on the internet that doesn't participate in these practices commonly referred to as behavioral targeting or retargeting" . . . "Note: We should not say we will never do these things."[24] That same year Brian Boland stated, "A key question we need to address sooner than later is whether we want to set ourselves apart from the market and specifically call out Google's practices or begin to look at ways we could

[20] FTC 2011 Complaint, ¶ 31.

[21] PALM-010934635: 4/13/2009.

[22] CONSUMER-FB-0000002215 at CONSUMER-FB-0000002216; Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 63-66 (2019).

[23] CONSUMER-FB-0000001494.

[24] PALM-011963339. Parent email is PALM-011963207.

Facebook's representation	Facebook's action
	leverage 3rd party data so that we are not left behind. I have been looking into the data approach as part of our 3rd party targeting, but there is a bigger question here around how we want to position ourselves against Google."[25] FB filed a patent application in Sept. 2011 for a "method . . . for tracking information about the activities of users of a social networking system while on another domain."[26]
Sheryl Sandberg prepared talking points for a Q&A in Davos, in a document dated January 22, 2013 titled "The Bible" "Q: Does Facebook use data from social plugins for the purpose of targeting ads? . . . No, we don't. We know that there are many other companies in our industry that do this. We don't think there is anything wrong with this as long as companies are clear with users that they do this and provide appropriate controls."[27]	See above.

Facebook also created "dossiers" of identifying and sensitive information on users and non-users, a fact it did not disclose and then subsequently disclaimed and stated it would rectify once some discovered the practice. Violet Blue, *Firm: Facebook's shadow profiles are 'frightening' dossiers on everyone*, ZD Net (June 24, 2013), https://www.zdnet.com/article/firm-facebooks-shadow-profiles-are-frightening-dossiers-on-everyone/. The chart below provides illustrative examples of this practice and Facebook's statements regarding it.

Facebook's representation	Facebook's action
Facebook stated it was not building behavioral profiles, and represented that it was complying with the obligations imposed by the 2011 consent decree.	A 2013 security bug exposed that Facebook had been combining contact information for people into "large dossiers." Facebook assures non-users that they can control information about them on Facebook.

[25] PALM0003232785: 2/22/2010.

[26] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 68 (2019).

[27] PALM-006761629 at -649.

Facebook's representation	Facebook's action
	But there was no way for a non-Facebook user to know their information was gathered or kept by Facebook. As of May 2022, non-users can go into Facebook to delete their contact information. However, Facebook has not said anything publicly, and is only available via a link that is embedded in an obscure help page. The link itself does not identify as a privacy tool, but reads, "Click here if you have a question about the rights you may have."[28] The tool asks non-users to submit their contact information so Facebook can confirm whether it has this data. Then non-users can request Facebook to delete it.
A document dated Dec. 6, 2012, intended to prepare Sandberg for a press interview, stated: Q: "Are you tracking people around the web? What are Facebook's views on tying real-world identity to web browsing history?" A: "We are not building behavioral profiles of people's activity across the web to target ads. Ads are served on Facebook like any other ad, and no user data is ever exchanged with partners or advertisers."[29]	Facebook was combining the information that users provided with off-platform data to create shadow profiles on users (for example, "uploading one public email address for an individual could reap a dozen additional pieces of contact information.") Due to a bug, the data was exposed for about a year.[30]

Also in 2013, Facebook stymied users' attempts to use tools like Do Not Track or adblockers to get Facebook to stop tracking, and then subsequently misrepresented that it had rectified the problem, as discussed in the illustrative examples below.

Facebook's representation	Facebook's action
Facebook assured users they could opt out of targeted ads on the Digital Advertising Alliance	The process of opting out was extremely inconvenient and had to be done for each device and browser. Even if successful in clicking through the options, the website was often down.

[28] https://www.businessinsider.com/facebook-has-hidden-tool-to-delete-your-phone-number-email-2022-10.

[29] PALM-007663967.

[30] Violet Blue, *Anger Mounts After Facebook's 'Shadow Profiles' Leak in Bug* (June 22, 2013), ZDNET, https://www.zdnet.com/article/anger-mounts-after-facebooks-shadow-profiles-leak-in-bug/; Violet Blue, *Security Firm: Facebook's Shadow Profiles are 'Frightening' Dossiers on Everyone* (June 24, 2013), ZDNET, https://www.zdnet.com/article/firm-facebooks-shadow-profiles-are-frightening-dossiers-on-everyone/.

Facebook's representation	Facebook's action
website (an industry alliance formed in response to FTC investigations).[31]	The opt-out solution only worked if a consumer set her browser security settings to permit third-party cookies, which was "the very mechanism that allows companies like Facebook to do what the consumer was now trying to avoid." Furthermore, if the user cleared their cookies (to get rid of tracking cookies), then that would have the effect of permitting tracking all over again.[32] In 2011, Facebook employees discussed the new ads product which let advertisers promote stories from newsfeed. Philip Zigoris stated, "its been decided that these 'sponsored stories' will not heed the social ads opt out rules going forward. BUT, in order to mitigate the risk of privacy-related shit storm, we are going to respect the social ads opt-out for users who are opted out *prior to launch*.we are also going to not show them these new kinds of ads. the thinking is that since these people are more privacy sensitive, we don't need to put this product in their face and garner unnecessary attention."[33]
Facebook provided their own privacy controls to permit users to opt out.	Facebook knew these settings were hard to find and insufficient. While discussing Project Bluebird, Joshua Grossnickle noted that "Another idea we discussed was a simplified control panel for ad preferences. One place people could see what data Facebook collects and control it. These setting are currently buried. The data control panel could include new options around data retention and be surfaced to all users at top of feed. Similar to our recent 3rd Party app control tool. People need to see and feel this in product. Sheryl and Chris were pushing to decouple the data control announcement from the ads-free announcement at F8. This seems unlikely to me

[31] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 76-78 (2019).

[32] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 76-(2019).

[33] PALM-008538403.

Facebook's representation	Facebook's action
	given Mark's reaction and the thin data controls we can offer."[34] Matt Steinfeld: "[W]e lack compelling proof points of the value [to consumers] created by our data collection" . . . " "Even if we do more controls etc. to take care of people's concerns above, I also think social may have a bigger you are the product problem than search because social is monetizing my content and data … which makes me think doubly that I am the product, or at least my content is (because it is). Overall my gut is that we need: • To do more to protect people's privacy "automatically", i.e. people don't have to do anything. This would be through shorter data retention policies etc. • A simpler control that does not reflect our product siloes. • And putting the control in front of people on a regular basis."[35]
Facebook represented that browser Do Not Track settings could help users to not be tracked. Sheryl Sandberg prepared talking points for a Q&A in Davos, in a document dated January 22, 2013 titled "The Bible". "Q: Does Facebook honor Do Not Track? . . . we promptly delete or anonymize information we get when people view pages that include social plugins, regardless of whether DNT is on."[36]	In 2013, Erin Egan, the chief privacy officer of Facebook, explained that Facebook would bypass consumer Do Not Track settings because Facebook does not track consumers for advertising purposes, in effect arguing that consumers do not understand what Do Not Track means. "We don't use that data for an advertising purpose," she emphasized. In 2014, after Facebook changed course and began tracking consumers for commercial purposes, Facebook simply continued to ignore consumers' Do Not Track signals.[37] In 2013, FB exposed data of opted-out users. Roi Tiger, VP Engineering, stated, "I just figured [sic] we're providing clickstream data for opted out users, which is very bad."[38]

[34] PALM-003543813.

[35] PALM-003574752.

[36] PALM-006761629 at -652-53.

[37] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 77-78 (2019).

[38] PALM-008936184.

Facebook's representation	Facebook's action
Facebook failed to disclose it was circumventing ad-blocking apps.	In Aug 2015, Apple announced iOS 9 would permit developers to introduce apps that enabled content blocking. When it released, the top downloads were for ad blockers, and by 2016, reports showed that one in five smartphone users (420 million people worldwide) were blocking ads while browsing on the mobile web. Facebook quickly engineered a way to circumvent users' installation of ad blockers. "Initially, Facebook prevented its public-facing pages from loading on user devices that had ad blockers installed. If consumers landed on forbes.com and Forbes prevented its page from loading, consumers could switch to a Forbes competitor to read news. With Facebook, consumers did not have any alternative product they could switch to. Then, in August of 2016, Facebook announced it had found a way to circumvent ad blockers entirely. Facebook 'flipped a switch on its desktop website that essentially renders all ad blockers . . . useless." At FB's Q3 2016 earnings call, Wehner even attributed half of the 18% YOY revenue growth in desktop ads as "largely due to our efforts on reducing the impact of ad blocking."[39]

In 2017, Facebook opted all users into facial recognition.

Facebook's representation	Facebook's action
Facebook announced the feature Tag Suggestion in 2010, which used facial recognition technology to assist users in tagging their Friends in photos or videos.[40] Facebook assured users they could opt out of this feature.	In 2017, Facebook replaced the Tag Suggestion feature with Face Recognition. While Tag Suggestion was automatically turned on for users, users had to affirmatively opt into Face Recognition. Facebook migrated users to Face Recognition, but approximately 60 million users were not migrated (leaving them under the default settings for Tag Suggestion). In April 2018, Facebook deleted all references to Tag Suggestions in its Policy and replaced it with Face Recognition. These 60 million users were thus deceived into thinking they were not participating

[39] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 78-80 (2019).

[40] DOJ Complaint ¶ 144.

Facebook's representation	Facebook's action
	in Face Recognition, when they were opted into participating in Tag Suggestion.[41]

Facebook also used data in more ways than it ever disclosed. For example, in 2011, Facebook sold users' shopping habits to advertisers using cookies called View Tags despite promises to not sell user data. The chart below provides illustrative examples of this practice and Facebook's public responses as compared to its private continuing practices.

Facebook's representation	Facebook's action
Facebook represented it used cookies, and permitted advertisers to use cookies, only for limited purposes.	Facebook used cookies, and permitted advertisers to use cookies, to track users even after they had logged off Facebook. Facebook also used cookies to track non-Facebook users. Facebook knew that it was illegal to use user data in advertisements. In a March 4, 2010 email from Allison Hendrix to sales, it was noted "it's illegal to do so without the consent of the user, and users get pissed when their name/image is used to hawk a product without their knowledge, so this is a big problem -currently we don't allow it at all, although we are exploring potentially opening this up (but that's not going to happen for a while) - mention the Ad Guidelines and how it also applies to Platform".[42] The cookies placed by advertisers were not reasonably necessary. In 2012, Facebook expanded its "View Tags" program, which "allows advertisers to track Facebookers across the Internet using cookies."[43] The cookies placed by advertisers were not permitted by the user. Facebook purported to allow users to opt out of targeted ads, but then circumvented their attempts to do so by 1) not allowing consumers to opt-out of off-site tracking and 2) ignoring consumers' explicit requests

[41] DOJ Complaint ¶ 153-54.

[42] PALM-012832296 (3/4/2010 email); PALM-012832297-PALM-012832313, at 2304 (attachment).

[43] CONSUMER-FB-0000001243 at CONSUMER-FB-0000001251.

Facebook's representation	Facebook's action
	through the Do Not Track option, and 3) circumventing installed ad blockers.[44] Sheryl Sandberg prepared talking points for a Q&A in Davos, in a document dated January 22, 2013 titled "The Bible". She notes that she wants to avoid the following point: "Although we do not 'sell' users' information, we should be careful about how broadly we make this commitment. First, we do provide aggregated insights to advertisers . . . Second, when users consent to disclosing their information (such as by making it public) we may make it available to marketers."[45] A 2011 document shows that Facebook placed cookies on users' computers to track them even after they had logged off.[46] On October 7, 2010, Barry Schnitt responded to Elliot Schrage's question regarding what they can and can't say regarding cookies: "For which of this information can we say we do not store it at all? . . . NONE. WE STORE ALL OF IT. . . For which of this information can we say we do not use it at all (versus not using it for monetization purposes). . . WE USE ALL OF IT…"[47] Two days later, on October 9, 2010, Elliot Schrage provides a recommended answer for potential questions regarding the use of cookies: "Unlike many other companies, Facebook does not use information from cookies to track people across the web and build profiles of them for advertising. In recent instances, when we were made aware that certain cookies were sending more information to us than we had intended, we fixed them immediately." Joel Kaplan explains that they're not allowed to make this statement: "Earlier this week, in preparing a response to

[44] Dina Srinivasan, The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy, 16 Berkeley Bus. L.J. 39, 76-77 (2019).

[45] PALM-006761629 at -649.

[46] PALM-007855708, Oct. 7, 2011.

[47] PALM-009498796: 10/7/2011

Facebook's representation	Facebook's action
	USA Today, Greg Stefancik…insisted that we could NOT use this specific formulation…For reasons Barry can explain better than I (but having to do with the inability to disable cookies that had already been dropped), we ultimately ended up going with the formulation included in your 'Long version' 'In recent instances, when we were made aware that certain cookies were sending more information than we had intended, we fixed OUR COOKIE MANAGEMENT SYSTEM immediately.' This was pretty heavily negotiated language…"[48]
Facebook's CTO, Bret Taylor, indicated in a Wall Street Journal piece on May 2011 that Facebook's use of cookies was "to protect users' Facebook accounts from cyber-attacks."[49] Sheryl Sandberg prepared talking points for a conference, including on cookies. It states, "Facebook did not use any information it should not have."[50] In a document dated December 2012 intended to prepare Sandberg for a press interview, Sandberg planned to say "Q: "Are you selling users' data to advertisers as a part of any of these products?" A: "No. We do not sell users' personal information. We provide services for marketers to more effectively reach their customers with relevant and personalized ads experiences."[51]	In 2012, Facebook began dropping cookies to "browsers of non-FB users." Erin Egan explained that "We've made representations to policymakers that we don't set cookies on the browsers of users who have never visited Facebook. Now we will be doing just that." Sheryl Sandberg wrote, "I really worry that being privacy focused has caused part of our current revenue problems."[52] In 2012, Facebook expanded its "View Tags" program, which "allows advertisers to track Facebookers across the Internet using cookies."[53]
In June 2014, Facebook issued a press release indicating that, with respect to its service of ads: "[t]oday, we learn about your interests primarily from the things you do on Facebook, such as Pages you like. Starting soon in the US, we will also include information from some of the	Facebook learns about user interests from inferred data, not from "things [users] do on Facebook."

[48] PALM-004129906: 10/9/2011.

[49] Amir Efrati, *'Like' Button Follows Web Users*, WALL ST. J. (May 18, 2011), https://www.wsj.com/articles/SB10001424052748704281504576329441432995616.

[50] PALM-005260799: 10/4/2011.

[51] PALM-007663967.

[52] PALM-008816198: 09/10/2012.

[53] CONSUMER-FB-0000001243 at CONSUMER-FB-0000001251.

Facebook's representation	Facebook's action
websites and apps you use. This is a type of interest-based advertising[.]"[54]	This announcement also came after 7 years of promises to not track and surveil customers.[55]
2016: "[W]e use all of the information that we have about you to show you relevant ads. We do not share information that personally identifies you (personally identifiable information is information such as a name or email address that can by itself be used to contact you or identify who you are) with advertising, measurement or analytics partners unless you give us permission."[56]	Facebook began disclosing that it uses all of the data it has on you to show relevant ads, but does not disclose what that data is.
In 2019, the FTC and Facebook entered into a Consent Decree. The FTC alleged that Facebook deceived users when the company shared the data of users' Facebook friends with third-party app developers, failed to monitor third party app developers, engaged in facial recognition against users' stated preferences, and misused information provided in the two-factor authentication process.	Facebook leadership discussed the launch of Viewpoints, and decided to delay it because of new requirements under the 2019 FTC Consent Decree. Erez Naveh recognized that Facebook's then-current practices—despite years of statements to the contrary—did not meet the bar required for adequate disclosure: "We are delaying the Facebook Viewpoints launch. . . A new FTC requirement made the technical bar of saying 'data is not used to target ads' much higher than before. . . In the new requirement, we also have to clearly disclose the appropriate statement in the product flows, either 'not used to target ads', or 'possible use for ads targeting'. Not mentioning it at all is not an option anymore."[57]

From approximately 2010 to 2018, Facebook sold direct access to Facebook data and APIs to certain third-party partners without telling users, through a feature called Instant Personalization, as demonstrated by the examples set forth in the below chart.

Facebook's representation	Facebook's action
Facebook assured consumers that they had control over their profile and who their profile was shared with.	Facebook automatically opted in users to Instant Personalization, which granted third parties access

[54] CONSUMER-FB-0000002348 at CONSUMER-FB-0000002379; Facebook, *Making Ads Better and Giving People More Control Over the Ads They See* (June 12, 2014), https://about.fb.com/news/2014/06/making-ads-better-and-giving-people-more-control-over-the-ads-they-see/

[55] Srinivasan article, at 70-71.

[56] PALM-008913162, Full Data Policy, dated September 29, 2016.

[57] PALM-012845007, 11/25/2019.

Facebook's representation	Facebook's action
	to users' information. This contradicted earlier assurances that users would have control. Facebook entered into agreements with third parties about use of consumers' data, but failed to disclose what these terms were. Users were only given five chances to disable Instant Personalization. Microsoft personnel stated about Instant Personalization on Bing, "Whenever you are visit Bing within a browser session where you are already logged in to Facebook, we authenticate you to Bing using Facebook. This is called Instant Peronalization [sic] . . . The first five times this happens for an individual user. A notification is displayed on screen allowing the user to disable the functionality. If they want to disable it subsequent to their fifth visit, they can go to the Facebook website and remove the Bing app."[58]
Facebook said it deprecated this feature in 2014.[59]	Certain parties still had access to users' data via an API well into 2018.[60]

From approximately 2011 to 2019, Facebook collected users' phone numbers as part of Two-Factor Authentication security measure, then sold this data to advertisers of Two Factor Authentication. This project was introduced in or around April 2011. E.g., PALM-012286784-PALM-012286786 ("Does the API exist? Yes, IP still exists."). This project was discovered on September 25, 2018. *See* Graham Cluley, Facebook's Two-Factor Authentication Announcement Raises Questions (Apr. 21, 2011), NAKED SECURITY, https://nakedsecurity.sophos.com/2011/04/21/facebook-two-factor-authentication-announcement-raises-questions. Additional publications corroborated this discovery in January 2019. *See* Kashmir Hill, *Facebook Is Giving Advertisers*

[58] MS-LIT_0000010895.

[59] Facebook last mentioned Instant Personalization in its Data Use Policy on January 20, 2015. *See* PALM-000791925-PALM-000791930, Data Use Policy subsection: Other websites and applications, dated Jan. 20, 2015.

[60] *E.g.*, PALM-012286784-PALM-012286786 ("Does the API exist? Yes, IP still exists.").

Access to Your Shadow Contact Information (Sept. 26, 2018), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051; *see also* https://mislove.org/publications/PII-PETS.pdf.

The chart below provides illustrative examples of this practice.

Facebook's representation	**Facebook's action**
Facebook represented it collected users' contact information for security reasons. It did not disclose any use of phone numbers obtained through Two Factor Authentication besides for authentication.	Facebook provided users' phone numbers and other contact information to advertisers.
In April 2011, Facebook announced the introduction of "two-factor" authentication.[120] In announcing the feature, Facebook said its purpose was to "help prevent unauthorized access to your account," because it was "additional security" that "helps confirm that it's really you trying to login."[61]	In 2018, it was revealed that FB is giving advertisers access to contact info that users did not consent to share publicly ("shadow contact information").[62] After the researchers' reports surfaced, Facebook acknowledged internally it used two-factor authentication phone numbers for advertising purposes: "[w]e will also look into feasibility and revenue impact of retiring use of two-factor authentication and alerts," but apparently denied that these practices were in conflict with its representations: "we have not made external commitments that they are not used for ads purposes."[63] Other internal Facebook documents acknowledge that "[i]f 2FA enrolees give us a new phone number, it may be used for purposes beyond account security (ex: PYMK)." The same presentation states,"[t]his does not meet the expectations of the market or the security/privacy community[.]"[64]
Facebook's later representations on its site indicated: "Why use two-factor authentication? Two-factor authentication is an industry best	In 2019, as part of a larger lawsuit against Facebook for violating the terms of its earlier 2011 FTC consent decree, the FTC and DOJ

[61] https://nakedsecurity.sophos.com/2011/04/21/facebook-two-factor-authentication-announcement-raises-questions/.

[62] https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051; https://mislove.org/publications/PII-PETS.pdf.

[63] PALM-004026741.

[64] PALM-008451978 at PALM-008451982, Mar. 25, 2019; PALM-008451986.

Facebook's representation	Facebook's action
practice for providing additional account security. We continue to encourage enabling two-factor authentication to add an extra layer of protection to your Facebook account."[65]	determined that Facebook engaged in deception regarding its use of phone numbers provided for two-factor authentication. As part of the settlement (which also involved Cambridge Analytica), Facebook paid a $5 billion fine. Facebook also "used those numbers for advertising purposes."[66]

From approximately 2010 to 2018, Facebook permitted all app developers—like Cambridge Analytica (founded in 2013)—unsupervised access to user and users' friends' data for political ends through Facebook's API. As early as 2010, internal discussions at Facebook revealed that apps had no oversight. PALM-009879439, Feb. 10, 2010. Major publications such as the New York Times broke this news on March 17, 2018. Sarah Todd & Dave Gershgorn, *The Cambridge Analytica Scandal is Wildly Confusing. This Timeline Will Help* (Mar. 29, 2018), QUARTZ, https://qz.com/1240039/the-cambridge-analytica-scandal-is-confusing-this-timeline-will-help/; Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions* (Mar. 17, 2018), N.Y. TIMES, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

The chart below provides illustrative examples of this practice and Facebook's statements to the contrary, then its statements about the practice, once disclosed.

Facebook's representation	Facebook's action
Facebook represents that users' data is protected from third parties and applications.	Facebook did not protect user data, instead permitting applications unsupervised access to users and users' friends' data. Facebook was discussing a model in which apps had no oversight from Facebook as early as 2009. An internal presentation by Ruchi Sanghvi to Zuckerberg proposed a new data permissions model that permits apps to track users and users' friends, with no oversight from FB. "Once a user gives an application their data; the application can… store the data… use it to target advertisements on their properties… applications are not forced to respect Facebook privacy…All

[65] https://www.facebook.com/notes/10157814548431886/.

[66] CONSUMER-FB-0000001261 at CONSUMER-FB-0000001265.

Facebook's representation	Facebook's action
	public data that in indexable is available to applications without user authentication… A user can grant applications access to private friend data excluding contact information…" The email attaches a deck that reflects this model and provides for 3 different interface options.[67] In 2010, emails revealed vulnerabilities that permit developers to publish user content that's more open than the users' default settings. Austin Haugen: "I've gotten some (very valid) concerns from the privacy folks about giving devs the ability to programmatically set the privacy on stream stories…it comes with the risk of devs not respecting user privacy and users being very surprised, especially as we make everyone stream search easier." Ray He "[T]he application is no way bound by our policies to not expose this user data on a third party website, allow it to be indexed, etc. Example: If I do something on Mafia Wars that results in a feed story, Zynga is under no obligation to not show my action to all their users (or everyone on the web) regardless of my feed privacy settings."[68] In the same year, employees discussed the new platform data policy. Kent Schoen: "The way I read the policy, user id can be passed to any third party (other than ad networks) without restriction or explicit user consent…That third party could then store the user id with their own cookie and via the FB API be able to lookup user information to include in their analytics." Ami Vora confirms: "this does enable the app devs to use the info they have for doing their own targeting on their own apps / sites, but they can't pass that targeting info anywhere else. [We don't believe this is a major competitive issue.]"[69]
Post-Consent Decree (2011 onward): Facebook acknowledges they shouldn't have shared users' data through their friends' profiles and represents	The Cambridge Analytica scandal revealed that this was false. Cambridge Analytica was developed in 2013 by data scientist Aleksandr Kogan. Cambridge Analytica collected and used

[67] PALM-007500874, PALM-007500876 - 1/22/2009.

[68] PALM-009879439, Feb. 10, 2010.

[69] PALM-003281987: 3/15/2010.

Facebook's representation	Facebook's action
they will give users control from that point forward. In 2014, Facebook specifically represented that it was ending third parties' unpermitted access to "Affected Friends" or "Friends of Friends" sharing. At Facebook's April 30, 2014, F8 conference, Zuckerberg announced, "Now we've heard really clearly that you want more control over how you're sharing with apps. . . . we've also heard that sometimes you can surprised when one of your friends shares some Azure data with an app. And the thing is we don't ever want anyone to be surprised about how they're sharing on Facebook and that's not good for anyone. So we're going to change how this works . . . And in the past, when one of your friend logged into an app, . . . the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so now that everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps."[70] In a public announcement on April 30, 2014, Facebook announced "three themes," including: "Putting people first: We've heard from people that they are worried about sharing information with apps, and they want more control over their data. We are giving people more control over these experiences so they can be confident pressing the blue button."[71]	the data of a Facebook users' friends. E.g., Cambridge Analytica could access the data of Person B—even if Person B never installed the app—so long as Person B was friends with Person A, who had the app installed. In 2013, Facebook realized they exposed data of opted-out users. Roi Tiger, VP Engineering, stated, "I just figured [sic] we're providing clickstream data for opted out users, which is very bad."[72] Friends of Friends (also known as "Affected Friends") data was precisely the data that Facebook was obligated to be truthful about after the 2011 FTC consent decree, and which Facebook said it was ending third-party access to in 2014. It was revealed in 2018 that Cambridge Analytica was able to access the data of some *87 million* Facebook users. In the immediate aftermath of news reporting regarding Cambridge Analytica in March 2018, Javier Olivan remarked "[n]ow we need to catch a bunch of the skeletons in the closet and fix them for realz. . ."[142] Javier Olivan also remarked: "We are going to have to do a lot around transparency and controls per all the threads popping up on CI use, SMS call logs, soft matching, PYMK, onavo . . . Can we start compiling all the 'skeletons' in one place?"[73] In a March 23, 2018 email entitled "CA response / cleaning up skeletons in the closet," Facebook employees coordinated "a formal workstream to coordinate the works 'clean up the skeletons' across the company[.]"

[70] https://singjupost.com/facebooks-ceo-mark-zuckerberg-f8-2014-keynote-full-transcript/?singlepage=1; PALM-005764422 at PALM-005764425–26.

[71] https://about.fb.com/news/2014/04/f8-2014-stability-for-developers-and-more-control-for-people-in-apps/.

[72] PALM-008936184.

[73] PALM-010027051.

Facebook's representation	Facebook's action
	Javier Olivan remarked that this work had already been underway, even prior to the Cambridge Analytica scandal: "About a year ago – we are [sic] reviewed all the privacy settings and experiences and evaluat[ed] them in terms of FB value and risk of PR/memes"[74] Facebook knew that there were apps that were trying to access the social graph. Edward O'Neil, in Dec. 9, 2013, stated "We've spent years fighting with birthday / horoscope apps that appeared to offer a small amount of user value in exchange for the graph."[75] This was part of a larger debate of who owned a users' friends' data – the user or the friend. David Poll argued: "[T]he 'my friends need to TOS the app' thing is basically a 'I'm going to kill this app' statement . . . I don't want all my friends to have to TOS." O'Neil disagreed, stating "I disagree – your friends birthdays aren't *yours* to take with you. We let you do that today, and it's created confusion along with regulatory / legal issues. It's also exactly what's gotten us intro [sic] trouble with Lulu." O'Neil stated: "It's also accrued a huge amount of value to developers at great expense to Facebook as a business." Poll: "If you want to give users a way to protect their data, it seems like the best way to do that is to give them a setting like 'app's can't see my data unless I've explicitly allowed it (by TOS-ing or through a whitelist)'." Poll: "[A]pps can't currently avoid asking for friends, nor do we actually push them to justify why they need the permission and disclose how they will use it." O'Neil: "Isn't the point most developers will take everything they can from the API – and hoping that they won't doesn't make it so." "Off FB, we should protect user info. Surveys show that people don't understand the data proxy model."

[74] PALM-009947206.

[75] PALM-000604575-PALM-000604583.

Facebook's representation	Facebook's action
	O'Neil: "if we can't enforce a policy, said policy doesn't actually exist". Poll: "Well, in many cases we can enforce a policy after the fact (e.g. we find out that someone is violating it in some bad way), but that does have lots of downside." O'Neil: "That's now pretty much all policy enforcement works – and without audit rights on developers' servers, we can't actually make sure they're not storing the data." In May 2018, an internal presentation listed among the "Top Ten Lessons Learned" was that "The world has changed – we** changed it" noting that We** includes FB, Google, YouTube, Reddit, Twitter "have an outsized influence in the world because we are the internet."[76]
In a May 7, 2015 interview with "Americas Quarterly," Javier Olivan stated: "Privacy is our number one priority. Giving people control over what they share is at the core of everything we do. We think about privacy from the time we start building a product until it goes out the door. We know that people will only trust Facebook if we do a good job of protecting their information."[77]	On December 11, 2015, The Guardian published an article entitled "Ted Cruz using firm that harvested data on millions of unwitting Facebook users." It stated, "Ted Cruz's presidential campaign is using psychological data based on research spanning tens of millions of Facebook users, harvested largely without their permission, to boost his surging White House run and gain and edge over Donald Trump and other Republican rivals."[78] After the Consent Decree, Facebook committed to no longer collecting and using the data of a Facebook user's friends. Facebook discovered by, at least, September 2015, that Cambridge Analytica accessed exactly this information.[79] Facebook represented that it demanded that Cambridge Analytica delete all friend data,[80] but still permitted it to continue to access and use the

[76] PALM-013147638.

[77] https://www.americasquarterly.org/fulltextarticle/interview-javier-olivan-facebook/

[78] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[79] PALM-009370309, Sept. 22, 2015.

[80] PALM-010316215 (Facebook employee Allison Hendrix interviewed Aleksandr Kogan, concluding "[h]is use and retention of friend information violates our data policies. There are other issues but that is the high level. We are continuing to investigate his use of information and determine next steps. We definitely plan to demand he delete all friend data.").

Facebook's representation	Facebook's action
	data (revealed by whistleblower Christopher Wylie).
On April 11, 2018, Politico published an article in which Zuckerberg refused to admit that Facebook violated the FTC consent decree (although he admits "I think we should have notified people [about Cambridge Analytica], because it would have been the right thing to do.").[81]	Internally, Facebook employees acknowledged Facebook's complicity. For example, Yul Kwon—Facebook's former Privacy Director—wrote to Deb Liu that he had previously in mid-2015 briefed Mark Zuckerberg "on the need to build a stronger and more centralized privacy & data use org." In the aftermath of the Cambridge Analytica revelations, Kwon "wonder[ed] how much of a better place we'd be in today if the proposal had been implemented three years ago."[82]
After the scandal, Facebook announced an "App Developer Investigation" to "review all of the apps that had access to large amounts of information before we changed our platform policies in 2014."[83]	Facebook executive Elliot Schrage appears to have described the App Developer Investigation as "a strawman approach to address the commitments we've made[.]"[84] Facebook employees referred to this as "our mistake" and stated, "We should avoid making any statements about the # of partners who could have accessed data. We didn't investigate that, so I don't know if that # is several dozen or hundreds." In 2019, a public update from Facebook's Vice President of Product Partnerships—Ime Archibong—acknowledged that Facebook had suspended "tens of thousands of apps[.]"[161] For example, Archibong's notes identified "myPersonality" as one app that "[h]ad access to friends' data"[85]
Post-Consent Decree (2019 onward): In 2019, the FTC and Facebook entered into a Consent Decree. The FTC alleged that Facebook deceived users when the company shared the data of users' Facebook friends with third-party app	Internally, Facebook recognized they were going to have to change their data practices after the Consent Decree. Message from Jonny Oser attaching slides laying out FTC Consent Order requirements and the

[81] PALM-009860465.

[82] PALM-010595431.

[83] CONSUMER-FB-0000002183.

[84] PALM-009854458.

[85] PALM-012139309.

Facebook's representation	Facebook's action
developers, failed to monitor third party app developers, engaged in facial recognition against users' stated preferences, and misused information provided in the two-factor authentication process. The parties settled for $5 billion.	seven privacy workstreams implemented to comply with the order. Page 1 - FTC Order requirements: "We cannot misrepresent our data practices, directly or by omission. . . We must design a new Privacy Program that addresses company-wide privacy risks and implements specific requirements, including a comprehensive risk assessment and robust Privacy SFN."[86]
In an October 12, 2017 interview with Axios, Sheryl Sandberg stated, "When you share on Facebook, you need to know that no one's going to steal our data. No one is going to get your data that shouldn't have it. That we're not going to make money in ways that would make you feel uncomfortable .... And that you're controlling who you share with.... Privacy for us is making sure that you feel secure, sharing on Facebook."[87]	Judge Davila held that, on a motion to dismiss, Facebook shareholders adequately alleged this statement was false when made. *See In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1015 (N.D. Cal. 2020).
In a March 16, 2018 post announcing the suspension of the Cambridge Analytica app, Facebook's then-Deputy General Counsel Paul Grewal (former Magistrate Judge) stated: "In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list. This is just one of the many ways we give people the tools to control their experience."[88]	Judge Davila held that, on a motion to dismiss, Facebook shareholders adequately alleged this statement was false when made. *See In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1015 (N.D. Cal. 2020).
In an April 4, 2018 edition of Facebook's "Hard Question" series that was posted online, Mark Zuckerberg said, with respect to Facebook: "the main principles are, you have control over everything you put on the service, and most of the content Facebook knows about i[s] because you chose to share that content with your friends and put it on your profile."[89]	Judge Davila held that, on a motion to dismiss, Facebook shareholders adequately alleged this statement was false when made. *See In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1015 (N.D. Cal. 2020).
On April 10, 2018, Mark Zuckerberg gave live oral testimony before the Joint Commerce and	Judge Davila held that, on a motion to dismiss, Facebook shareholders adequately alleged this statement was false when made. *See In re*

[86] PALM-012843981 & PALM-012843983, 07/19/2019.

[87] https://www.axios.com/exclusive-interview-with-facebooks-sheryl-sandberg-1513306121-64e900b7-55da-4087-afee-92713cbbfa81.html.

[88] https://about.fb.com/news/2018/03/suspending-cambridge-analytica/.

[89] https://about.fb.com/news/2018/04/hard-questions-protecting-peoples-information/.

Facebook's representation	Facebook's action
Judiciary Committees for the United States Senate, stating: (a) "This is the most important principle for Facebook: Every piece of content that you share on Facebook, you own and you have complete control over who sees it and -- and how you share it, and you can remove it at any time. That's why every day, about 100 billion times a day, people come to one of our services and either post a photo or send a message to someone, because they know that they have that control and that who they say it's going to go to is going to be who sees the content. And I think that that control is something that's important that I think should apply to -- to every service." (b) "That's what the [Facebook] service is, right? It's that you can connect with the people that you want, and you can share whatever content matters to you, whether that's photos or links or posts, and you get control over it." (c) "The two broad categories that I think about are content that a person is[sic] chosen to share and that they have complete control over, they get to control when they put into the service, when they take it down, who sees it. And then the other category are data that are connected to making the ads relevant. You have complete control over both." (d) "Every person gets to control who gets to see their content." (e) "But, Senator, the -- your point about surveillance, I think that there's a very important distinction to draw here, which is that when -- when organizations do surveillance[,] people don't have control over that. But on Facebook, everything that you share there[,] you have control over."[90]	*Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1015 (N.D. Cal. 2020).
On April 11, 2018, Mark Zuckerberg testified before the U.S. House of Representatives' Energy and Commerce Committee, making the following representations: (a) "[. . .] on Facebook, you have control over your information."	This statement was false when made, for the reasons and based on the additional evidence set forth within this response.

[90] https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/.

Facebook's representation	Facebook's action
(b) "[. . .] every single time that you share something on Facebook or one of our services, right there is a control in line, where you control who -- who you want to share with." (c) "Congresswoman, giving people control of their information and how they want to set their privacy is foundational to the whole service [on Facebook]. It's not just a – kind of an add-on feature, something we have to . . . comply with. . . . all the data that you put in, all the content that you share on Facebook is yours. You control how it's used.[91]	
In Facebook's June 29, 2018 written responses to Congressional inquiries, Facebook represented: • "[w]e already show people what apps their accounts are connected to and allow them to control what data they've permitted those apps to use." • "Privacy is at the core of everything we do, and our approach to privacy starts with our commitment to transparency and control—to helping people understand how their data is collected and used, and to giving them meaningful controls. Our approach to control is based on the belief that people should be able to choose who can see what they share and how their data shapes their experience on Facebook and should have control over all data collection and uses that are not necessary to provide and secure our service People can control the audience for their posts and the apps that can receive their data when they login with Facebook."[92]	This statement was false when made, for the reasons and based on the additional evidence set forth within this response.

From 2007 to 2019, Facebook "whitelisted" certain software and hardware partners through agreements permitting access to user and users' friends' data through private APIs. Facebook has had private APIs (also called "Extended APIs," these are APIs whose access control is maintained by partnerships) since the invention of Facebook. *See* Deposition of Konstantinos Papamiltiadis, Feb.

[91] https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee/.

[92] https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/House%20QFRs.compressed.pdf.

23, 2021, *In re Facebook, Inc., Consumer Privacy User Profile Litigation*, No. 3.18-md-02843-VC, Dkt. 1038-12, at p. 220-21, 226. In 2018, these undisclosed relationships were revealed by the New York Times. Gabriel J.X. Dance, Michael LaForgia, & Nicholas Confessore, *As Facebook Raised a Privacy Wall, IT Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html; PALM-008743234 (internal collection of coverage of the event). Facebook's internal discussion states certain partners continued to have access to types of friends' data in 2019. PALM-008774330 (July 2019 email chain, estimating that 27 apps and 15 partners actually accessed data, but that the number of partners who could have accessed data is unknown). As of 2009, whitelisted mobile apps were kept in a table in Hive, titled tmp_msharon_native_clients. PALM-010099214, 7/5/2009. An updated list of API Whitelist Maps was catalogued in May 2010. PALM-001280609-PALM-001280667.

Illustrative examples of the bases for this contention are stated in the chart below.

Facebook's representation	**Facebook's action**
Pre-Consent Decree (pre-2011): Facebook represents that users' data is protected from third parties and applications.	Facebook did not protect user data, instead permitting certain partners access to users and users' friends' data. Under a so-called "Private Extended API Addendum," Facebook agreed to make available in some instances "Private Extended APIs," which are "a set of API's and services provided by FB to Developer that enables Developer to retrieve data or functionality relating to Facebook that is not generally available under Platform, which may include persistent authentication, photo upload, video upload, messaging and phonebook connectivity."[93] There were approximately 150 companies with special deals with Facebook that granted them access to data. The earliest of these deals were dated 2010, all were active in 2017, and some were still active in 2018.[94]

[93] PALM-000079637 at PALM-000080401–02.

[94] Gabriel J.X. Dance, Michael LaForgia, & Nicholas Confessore, *As Facebook Raised a Privacy Wall, IT Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

Facebook's representation	Facebook's action
	"Facebook allowed Microsoft's Bing search engine to see the names of virtually all Facebook users' friends without consent, the records show, and gave Netflix and Spotify the ability to read Facebook users' private messages. The social network permitted Amazon to obtain users' names and contact information through their friends, and it let Yahoo view streams of friends' posts as recently as this summer, despite public statements that it had stopped that type of sharing years earlier."[95] On March 25, 2010, FB personnel had meetings with Yahoo about accessing Yahoo data: "We asked many, many times why Yahoo cannot give us access to sent mail as part of contact importer and why they don't automatically add people you email to your contacts. Ash had previously explained that the reason for this was they'd decided it wasn't a good user experience. What Ash didn't go into, which Sam did, is that Yahoo got badly burned on the privacy front in the 2000-2001 time frame and is now extremely conservative on this. He went on to explain how people do things on Yahoo that they want to keep extremely private (personals, membership in pornographic groups etc.) and that they do so with multiple identities and email accounts, members. This drove home further for me why our mission of making the world more open and connected makes so much sense: transparency and openness are civilizing forces in that people are less likely to do things they're not proud of if all their friends can see them do it.[96]
Post-Consent Decree (2011 onward): Facebook acknowledges they shouldn't have shared users' data through their friends' profiles and represents they will give users control from that point forward.	Friends of Friends (also known as "Affected Friends") data was precisely the data that Facebook was obligated to be truthful about after the 2011 FTC consent decree, and which Facebook said it was ending third-party access to

[95] Gabriel J.X. Dance, Michael LaForgia, & Nicholas Confessore, *As Facebook Raised a Privacy Wall, IT Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

[96] PALM-003025305-PALM-003025306.

Facebook's representation	Facebook's action
In 2014, Facebook specifically represented that it was ending third parties' unpermitted access to "Affected Friends" or "Friends of Friends" sharing. At Facebook's April 30, 2014, F8 conference, Zuckerberg announced, "Now we've heard really clearly that you want more control over how you're sharing with apps. . . . we've also heard that sometimes you can surprised when one of your friends shares some Azure data with an app. And the thing is we don't ever want anyone to be surprised about how they're sharing on Facebook and that's not good for anyone. So we're going to change how this works . . . And in the past, when one of your friend logged into an app, . . . the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so now that everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps."[97] In a public announcement on April 30, 2014, Facebook announced "three themes," including: "Putting people first: We've heard from people that they are worried about sharing information with apps, and they want more control over their data. We are giving people more control over these experiences so they can be confident pressing the blue button."[98]	in 2014. Cambridge Analytica revealed in 2018 that all developers could access user data. Facebook also gave certain partners special access by agreement. In 2014, FB carved out exceptions for certain apps. Apps "Badoo" and "Hot or Not" wrote Facebook in 2014 "to explain the hugely detrimental effect that removing friend permissions will cause to our hugely popular (and profitable) applications." In January 2015, Facebook's Konstantinos Papamiltiadis responded: "We have now approval from our internal stakeholders to move ahead with a new API – working name Hashed Anon All Friends API. The new API as well as the relevant docs will be ready next week. How this API would work. . . For each of the FB logged in users, the API will return: *FBID*s: App friends that logged in before your migration to V2: App Scoped IDs: App friends that logged in after your migration to V2: *Anonymous one-way hashed IDs*: Non-app friends . . . This API will hopefully let you . . . determine which non-app friends to recommend to a given user[.]"[99] Facebook knew, as it acknowledged in 2014, that its whitelisting practice could invite regulatory scrutiny. "The other reason I'd rather not whitelist them is that the Capabilities Tool . . . is being heavily scrutinized by the FTC auditing process."[100] In a 2015 email to Facebook, Netflix referred to its "be[ing] whitelisted for getting *all* friends, not just connected friend[.]"[101]

[97] https://singjupost.com/facebooks-ceo-mark-zuckerberg-f8-2014-keynote-full-transcript/?singlepage=1; PALM-005764422 at PALM-005764425–26.

[98] https://about.fb.com/news/2014/04/f8-2014-stability-for-developers-and-more-control-for-people-in-apps/.

[99] PALM-004694014.

[100] PALM-000699851.

[101] PALM-000722384.

Facebook's representation	Facebook's action
	In a 2015 email with AirBnB, Facebook's Konstantinos Papamiltiadis explained that AirBnB could obtain access to certain friends data, but that it "will need to sign an agreement that would allow you access to this API."[102] After news of FB's software partners broke in 2018, Facebook executives circulated press clippings, stating "API hygiene: In some cases, our winding down of specific features did not translate into an automatic winding down of API access. This has been held up as proof positive that Facebook's management of these partnerships was lax, and we've faced lots of questions on why this is." . . . "we have faced calls to share more precise information about the specific permissions people granted to partners like Spotify and Netflix for messaging, and we've been working to confirm as much as we can (though we're lacking details to push back on this more forcefully)."[103] Facebook also acknowledged that these events regarding certain partners were contrary to earlier public representations. For example, in a July 23, 2019 email labeled "[CONFIDENTIAL, DO NOT FORWARD]," Facebook employees stated: "We previously announced last year that we had stopped supporting many of these partner integrations, but have discovered that some of these integrations were still accessing data."[104] In July 2019, Facebook agreed to provide this access to one app Tobii indefinitely.[105] On July 17, 2019, Konstantinos Papamiltiadis stated that Bing also "had access to friends data in 2015," which was classified as a device integration. As of 2019, it no longer had access.[106]

[102] PALM-000737803 at PALM-000737804.

[103] PALM-008743234.

[104] PALM-004608388.

[105] PALM-004608388 (July 2019 email chain).

[106] PALM-004951572-PALM-004951574, 7/17/2019.

Facebook's representation	Facebook's action
	On July 17, 2019, internal FB strategy discusses how to frame the issue to Microsoft. "Narrative to Microsoft: . . .we discovered last month that some apps that we thought we had cut access to were pinging FB APIs . . .MSFT was one of those companies, and a use case that we didn't disclose in prior public and on the record disclosers [sic] ~~to FTC or Congress~~" (strikethrough in original).[107] On July 18, 2019, Konstantinos Papamiltiadis discussed with other employees that data certain companies were given, e.g. Microsoft (Windows Phone and Skype) had certain integrations. Papamiltiadis stated, "skype could enable people to make calls even if they only have access to friends list . . . we gave them access to bdays, newsfeed, etc . . . to give people triggers/reasons to call their friends." The employee Papamiltiadis is in conversation with says, "But Tobii and Apple and Playstation continue to be able to access friends data now, right? (And Amazon did in 2019 until it was deprecated, right?) . . . Actually, forget it—I'll just make the caveat cover the whole thing."[108] On July 20, 2019, Papamiltiadis stated internally: "We have to announce because we [have] evidence that contradicts statements we made in public last year that device integrations will be wind [sic] down and more apps would have access to friends data . . . beyond Dec 2018" and "[w]e have to mention Microsoft by name as one of their apps continued to have access to friends data in 2019"[109] On July 23, 2019, in context of crafting press release about apps that continued to have access to Friends Data, even after Facebook's contrary statements in 2018, Facebook employees cautioned: "We should avoid making any statements about the # of partners who could have accessed data. We didn't investigate that, so I

[107] PALM-004617272-PALM-004617273, 7/19/2019.

[108] PALM-004617402; see also PALM-008779685.

[109] PALM-003961720-PALM-003961721, 7/20/2019.

Facebook's representation	Facebook's action
	don't [know] if that # is several dozen or hundreds."… "For did access, our latest count is 27 apps / 15 partners who actually accessed data. But that includes ones we knew about and were cool with, like Apple/Tobii/Amazon."[110] On July 23, 2019, an internal work chat acknowledged that "Skype had access to friends' emails and phone #'s . . . We know Skype had the ability to get a friend's phone and email (mobile_contact capa). We know it pulled User's contact info. It's hard to determine if it was pulling it for friends, but based on why it existed, we can assume it was."[111] In the aftermath, strategic considerations were made for withdrawing these permissions, e.g. how competitive the third party was to Facebook. On August 21, 2013, Papamiltiadis discussed strategy around granting third parties access to friends' permissions. He has a list of "40k+ apps that request and make use of the friends_permissions." He looks at the top 250. He puts them into categories, one of which is "Strategic." "From MSFT, to Yahoo!, to Pinterest, Path, Klout and the likes. Some of them should be obvious not [sic] have access such as Myspace, Twitter, Youtube, etc. In particular for Strategic partners we should use the framework developed by Jackie. RECOMMENDATION: User [sic] Jackie's framework." Jackie's framework is that of Jackie Chang, he recommends doing a risk assessment, including "Competitive/Not Useful to FB: Key integrations that are competitive or drive little value to fb. Good that we're removing, but may need some additional considerations on wind down time. Major Business Disruption / Kill: Noticeable integrations whose whole business is built on stream or friend data. Should be part of PR flag."[112]

[110] PALM-008774330.

[111] PALM-004625943-PALM-004625945.

[112] PALM-000076457.

Facebook's representation	Facebook's action
	On August 27, 2013: Sam Lessin emails Ime Archibong and Konstantinos Papamiltiadis and Kelly Jang: "[M]y gut is pretty strongly [sic] that we should shut down access to friends on lifestyle apps… because we are ultimately competitive with all of them and they leak data…"[113] In December 5, 2018, internal discussions between FB employees stated that some third parties could read and send all messages of FB users. ""When you say Spotify can read and send messages, are you referring specifically to the message sent from Spotify? Or ALL messages between the two people?" .. "all . . . titan_api is what gates access to the collection of messaging apis. Most messaging functionality like sending messages or reading messages sent to your users will be possible with it." Konstantinos Papamiltiadis stated though that it was not still live.[114] Facebook also granted special access to certain hardware/OEM partners As of 2008, FB internally reported that it had 108 linking deals, including mobile and handset OEMs (Rim/Blackberry, Nokia, iPhone, Palm, Motorola, SEM).[115] Facebook "separately maintained data sharing partnerships with at least 60 device makers and a 'small number' of partners to whom it also continued to provide access." For example, they made a deal with Apple in 2012, Microsoft in 2012, and Nuance Communications in 2015,[116] Amazon, BlackBerry, and Samsung, among others. "Facebook allowed the device companies access to the data of users' friends without their

[113] PALM-000076457.

[114] PALM-ADI-0000581918, 12/5/2018.

[115] PALM- 003203384, 11/16/2008.

[116] *Facebook Granted Custom Access to User Data to Selected Companies*, PRIVACY INTERNATIONAL (June 8, 2018), https://privacyinternational.org/examples/2701/facebook-granted-custom-access-user-data-selected-companies.

Facebook's representation	Facebook's action
	explicit consent, even after declaring that it would no longer share such information with outsiders. Some device makers could retrieve personal information even from users' friends who believed they had barred any sharing[.]" While Facebook sought to distinguish the "device makers" from the rogue app developers that had access to data, The New York Times conducted "tests" which "showed that the partners requested and received data in the same way other third parties did. The FTC's former Chief Technologist, Ashkan Soltani, described Facebook's making available this data to device manufacturers as follows: "It's like having door locks installed, only to find out that the locksmith also gave keys to all of his friends so they can come in and rifle through your stuff without having to ask you for permission[.]"[117] Facebook internally acknowledge that their public statements were misleading. In July 2019, Konstantinos Papamilitadis stated, "We have to announce because we [have] evidence that contradicts statements we made in public last year that device integrations will be wind [sic] down and more apps would have access to friends data . . . beyond Dec 2018" and "[w]e have to mention Microsoft by name as one of their apps continued to have access to friends data in 2019."[118]
In a May 7, 2015 interview with "Americas Quarterly," Javier Olivan stated: "Privacy is our number one priority. Giving people control over what they share is at the core of everything we do. We think about privacy from the time we start building a product until it goes out the door. We know that people will only trust Facebook if we do a good job of protecting their information."[119]	See above.

[117] CONSUMER-FB-0000001857.

[118] PALM-003961720 (July 2019 email chain).

[119] https://www.americasquarterly.org/fulltextarticle/interview-javier-olivan-facebook/.

Plaintiffs incorporate by reference their response to Meta's Interrogatory No. 6 and Meta's Interrogatory No. 21.

Consumer Plaintiffs further state that *Am. Pro. Testing Serv., Inc. v. Harcourt Brace Jovanovich Legal & Prof. Publ., Inc.*, 108 F.3d 1147 (9th Cir. 1997) did not concern material omissions and the factors listed are not applicable to omissions. Consumer Plaintiffs have already identified the relevant omissions and have no duty to prove falsity of an omission or reliance. Consumer Plaintiffs will address the evidence of materiality and lack of knowledge at the proper time in this case.

Consumer Plaintiffs continue to gather information, documents, and testimony regarding Facebook's representations and omissions and reserve the right to amend these responses after the close of fact discovery.

INTERROGATORY NO. 23:

For each of the practices You allege Meta failed to disclose, including but not limited to any of the omissions that You identified in Your response to Meta's Interrogatory No. 6 and any of the practices that You identified in Your response to Meta's Interrogatory No. 21, describe in full and complete detail (including but not limited to by identifying all facts, Documents, and witnesses that relate to Your contention) the facts You allege gave rise to a duty to disclose such practices.

RESPONSE TO INTERROGATORY NO. 23:

Consumer Plaintiffs object to this Interrogatory on the grounds set forth in detail above in their General Objections. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds it is entirely duplicative of Interrogatory Nos. 6-8, and 21. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds that it calls for a legal conclusion. Consumer Plaintiffs further specifically object to this Interrogatory on the grounds that it is overbroad, unduly burdensome, and disproportionate to the needs of the case, including in requesting that Consumer Plaintiffs "identify[] all facts, Documents, and witnesses that relate to [Consumer Plaintiffs'] contention." Consumer Plaintiffs do not agree to identify every fact, document, or witness that "relates" to Consumers' claims, and are not obligated to do so under the relevant Rules and law

from its users certain of their data.[120] Consumer Plaintiffs allege that contrary to Facebook's representations regarding the data that Facebook collected from its users and the uses to which Facebook put that data, Facebook collected more data from its users (Consumer Plaintiffs and other members of the putative Consumer Class) and put their data to additional, non-disclosed uses. Consumer Plaintiffs assert that Facebook obtained monopoly power by deceiving the market about its data collection and use practices. Consumer Plaintiffs further assert that, once obtained, Facebook's monopoly power allowed Facebook to continue engaging in these additional, non-disclosed data collection and use practices. Cf. CONSUMER-FB-0000000641 at CONSUMER-FB-0000000692 (report by United States House of Representatives Antitrust Subcommittee explaining that "a platform's ability to maintain strong networks while degrading user privacy can reasonably be considered equivalent to a monopolist's decision to increase prices or reduce product quality."). Consumer Plaintiffs' and the Consumer Class' damages are thus the difference between the compensation that Facebook actually provided for the data that Facebook collected from them and put to use, and the compensation that they should have received for that data in a competitive world. *See, e.g.*, Consumer Complaint, ¶¶ 10–11, 223–29; Klein, Dkt. 109 at 1, 5, 29–30. That compensation could have taken the form of either direct monetary payments, or in-kind consideration. See, e.g., CONSUMER-FB-0000002411 at CONSUMER-FB-0000002415

[120] The monetary value of this in-kind transaction between Facebook, on the one hand, and users, on the other, is well recognized. For example, Facebook's own co-founder, Chris Hughes, has explained that Facebook "is not actually free, and it certainly isn't harmless. . . . We pay for Facebook with our data and our attention, and by either measure it doesn't come cheap." CONSUMER-FB-0000002291 at CONSUMER-FB-0000002298. Regulators have also recognized as much. For example, a 2019 report commissioned by the Digital, Culture, Media and Sport Committee of the United Kingdom House of Commons explains that "[i]n portraying itself as a free service, Facebook gives only half the story." CONSUMER-FB-0000000009 at CONSUMER-FB-0000000050. Similarly, Rohit Chopra—then-Commissioner of the Federal Trade Commission (now the Director of the Consumer Financial Protection Bureau)—has explained, with respect to Facebook, "[w]e are paying with our data, that valuable data[.]" CONSUMER-FB-0000000426 at CONSUMER-FB-0000000469, CONSUMER-FB-0000000544. Reporters have likewise recognized the monetary value of this transaction. *See, e.g.,* CONSUMER-FB-0000002601 at CONSUMER-FB-0000002606 ("As for Facebook being a 'free' service – a point Zuckerberg is most keen to impress . . . 'if it's free you're the product'."). And, a panel of economists—led by Jason Furman, Former Chair of the White House Council of Economic Advisers—have similarly made clear that "[c]onsumers may pay for services implicitly through their personal data or their attention." CONSUMER-FB-0000002429 at CONSUMER-FB-0000002523.